JOURNAL OF NUMBER THEORY 9, 218–228 (1977)

Quadratic Function Fields with Invariant Class Group

DANIEL J. MADDEN

Department of Mathematics, Ohio State University, Columbus, Ohio 43210

Communicated by H. Zassenhaus

Received November 20, 1976

Emil Artin studied quadratic extensions of $k(x)$ where k is a prime field of odd characteristic. He showed that there are only finitely many such extensions in which the ideal class group has exponent two and the infinite prime does not decompose. The main result of this paper is: If K is a quadratic imaginary extension of $k(x)$ of genus G, where k is a finite field of order q, in which the infinite prime of $k(x)$ ramifies, and if the ideal class group has exponent 2, then $q = 9$, 7, 5, 4, 3, or 2 and $G \leqslant 1$, 1, 2, 2, 4, and 8, respectively. The method of Artin's proof gives $G \leqslant 13$, 9, and 9724 for $q = 7$, 5, and 3, respectively. If the infinite prime is inert in K, both the methods of this paper and Artin's methods give bounds on the genus that are roughly double those in the ramified case.

1. INTRODUCTION

The main object of this paper is to use the techniques and the results of [2] in a study of quadratic extensions of $k(x)$. In his dissertation Emil Artin studied the arithmetic and analytic theory of quadratic extensions of $k(x)$ where k is a field of prime order. His approach to this subject is a complete analogy to the theory of algebraic number fields, and, for this reason, he separated these extensions into two classes, real and imaginary, depending upon (in the terminology of this paper) the decomposition of the infinite prime of $k(x)$ in the extension. This distinction can be extended to arbitrary extensions of $k(x)$.

DEFINITION. *If K is an extension of $k(x)$ for which there is only one prime divisor that lies over the infinite prime of $k(x)$, then K is called an imaginary extension of $k(x)$; otherwise K is a real extension of $k(x)$.*

Notice that any prime of $k(x)$ of degree 1 may act as the infinite prime since

$$k(x) = k(1/(x + a)), \qquad \text{for any } a \in k.$$

ISSN 0022-314X

A field K is said to be a totally imaginary extension of $k(x)$ if no prime of degree 1 in $k(x)$ splits in K.

In the course of his study of quadratic extensions of $k(x)$, Artin discussed the problem of classifying all imaginary extensions of $k(x)$ which have one class per *Geschlecht*, i.e., in which the ideal class group has exponent 2. He proved that the number of such fields is finite; more precisely, he showed that in any such field $| k | = q = 3, 5$, or 7 and that (in the terminology of this paper) the genus is bounded. The techniques developed in the present paper can be used to remove the condition that k be a prime field and to substantially improve the bounds on the genus. However, for the sake of simplicity, this paper will, for the most part, be confined to those imaginary extensions in which the infinite prime ramifies. In this case the methods of Artin give that when $| k | = q = 3, 5$, and 7 the genus of the extension must be less than or equal to 9724, 9, and 13, respectively. The results obtained through the methods of this paper are given in the form of

THEOREM 1. *If K is a quadratic imaginary extension of $k(x)$ of genus G, where k is a finite field of order q, in which the infinite prime of $k(x)$ ramifies, and if the ideal class group of K has exponent* 2, *then*:

(i) $q = 9, G = 1$;
(ii) $q = 7, G = 1$;
(iii) $q = 5, G \leqslant 2$;
(iv) $q = 4, G \leqslant 2$;
(v) $q = 3, G \leqslant 4$; *or*
(vi) $q = 2, G \leqslant 8$.

The study of congruence function fields with ideal class exponent 2 is made by first considering those fields with null class exponent 2. If K is a quadratic imaginary extension of $k(x)$ in which the ideal class group has exponent 2, then, since the null class group of an imaginary extension is a subgroup of the ideal class group (see [1, pp. 246–247]), the null class group must either have exponent 2 or be of order 1. Madan and Queen [3] have shown that there are only two cases in which a quadratic extension of $k(x)$ has class number 1 and $G > 1$. In both of these cases, $q = 2$ and $G = 2$. Since it is assumed that the infinite prime $k(x)$ ramifies, the connection is even simpler; for then, the ideal class group and the null class group are identical. Therefore, Theorem 1 follows immediately from the following two theorems.

THEOREM 2. *If K is a quadratic extension $k(x)$ for which the null class group has exponent* 2, *then K is an imaginary extension of $k(x)$ for a suitable choice of x. In fact, if K has genus greater than or equal to* 2, *then K is a totally imaginary extension of $k(x)$.*

THEOREM 3. *Let K be a quadratic extension of $k(x)$ with genus G, where k is a finite field with q elements and in which not all the primes of degree 1 in $k(x)$ are inert. If the null class group of K has exponent 2, then*

(i) $q = 9$, $G = 1$;
(ii) $q = 7$, $G = 1$;
(iii) $q = 5$, $G \leqslant 2$;
(iv) $q = 4$, $G \leqslant 2$;
(v) $q = 3$, $G \leqslant 4$; or
(vi) $q = 2$, $G \leqslant 8$.

The restriction in Theorem 3 that not all the primes of degree 1 in $k(x)$ are inert in K is imposed only for the sake of convenience and, as we shall see, is redundant for $q = 7$ and $q = 9$. Without this restriction, the methods used here give bounds on the genus that are roughly double those in Theorem 3. This also is a substantial improvement over the bounds obtained through Artin's method.

2. NORMS OF INTEGRAL ELEMENTS IN IMAGINARY EXTENSIONS

With the definition of imaginary extensions, Theorems 4, 5 and 10 in [2] take on a special meaning. In an imaginary extension K of $k(x)$, there is only one prime $\mathfrak{P}_\infty$ which lies over the infinite prime $\mathfrak{p}_{1/x}$ of $k(x)$. Then

$$\begin{aligned} \deg N(\alpha) &= -v_{\mathfrak{p}_{1/x}}(N(\alpha)) \\ &= -(1/e_\infty)\, v_{\mathfrak{P}_\infty}\Big(\prod_{\sigma \in GAL(K/k(x))} \sigma(\alpha)\Big), \end{aligned}$$

where e_∞ is the ramification index of $\mathfrak{P}_\infty$, (1)

$$\begin{aligned} &= -(1/e_\infty) \sum_{\sigma \in GAL(K/k(x))} v_{\sigma\mathfrak{P}_\infty}(\alpha) \\ &= -(p^n/e_\infty)\, v_{\mathfrak{P}_\infty}(\alpha), \qquad p^n = [K : k(x)]. \end{aligned}$$

Thus, in imaginary extensions, Theorems 4, 5, and 10 in [2] can be used to give bounds on the degrees of norms of primitive integral elements. In particular this gives

THEOREM 4. *Let k be a finite field of order q, and let K be an imaginary extension of $k(x)$ with genus G.*

(A) *If K is a cyclic geometric extension of $k(x)$ of prime power degree for a prime other than the characteristic, then, for any $\alpha \in K$ which is both a primitive element for the extension $K/k(x)$ and integral over $k[x]$,*

$$\deg N(\alpha) \geqslant \deg\left(\prod p_i(x)\right),$$

where the product is taken over all the ramified polynomial primes of $k(x)$.

(B) *If K is a geometric Artin–Schreier extension of $k(x)$, then, for any $\alpha \in K$ which is both a primitive element for the extension $K/k(x)$ and integral over $k[x]$,*

$$\deg N(\alpha) \geqslant \deg\left(\prod p_i(\lambda)\right) + \max\{\deg n(x), \deg d(x)\},$$

where the product is taken over all the ramified polynomial primes of $k(x)$ and where $n(x)$ and $d(x)$ are defined by the generating equation of K,

$$y^p - y = n(x)/d(x).$$

(C) *If K is a geometric quadratic extension of $k(x)$, then, for any $\alpha \in K$ which is integral over $k[x]$ but not in $k[x]$,*

$$\deg N(\alpha) \geqslant 2G + 1.$$

Proof. (A) If $\{\theta_i\}$ is the fundamental basis constructed in Theorem 3 of [2], then

$$\alpha = a_0(x)\,\theta_0 + a_1(x)\,\theta_1 + \cdots + a_{p^n-1}(x)\,\theta_{p^n-1},$$

and

$$v_{\mathfrak{P}_\infty}(\alpha) = \min_{0 \leqslant j < p^n} \{v_{\mathfrak{P}_\infty}(a_j(x)\,\theta_j)\} \leqslant \min_{0 \leqslant j < p^n} \{v_{\mathfrak{P}_\infty}(\theta_j)\}.$$

This gives

$$v_{\mathfrak{P}_\infty}(\alpha) \leqslant -(e_\infty/p^n) \sum \deg p_i(x),$$

where the sum is taken over all the ramified primes of $k(x)$. Thus, plugging this into (1) gives

$$\deg N(\alpha) \geqslant \deg\left(\prod p_i(x)\right).$$

But this proves the theorem only when k contains the p^nth roots of 1; however, just as Theorem 4 extends to Theorem 5 in [2], it is possible to drop this condition on the roots of unity.

(B) Since K is an imaginary extension, (1) gives

$$\deg N(\alpha) = -(p/e_\infty)\, v_{\mathfrak{P}_\infty}(\alpha).$$

Then,

$$v_{\mathfrak{P}_\infty}(\alpha) \leqslant -(e_\infty/p)\left(\sum_{i=1}^{l} (\lambda_i + 1) \deg p_i(x) + \lambda_\infty\right),$$

where

$$y^p - y = n(x)/d(x)$$

is the generating equation of K over $k(x)$. Thus

$$\deg N(\alpha) \geqslant \sum_{i=1}^{l} (\lambda_i + 1) \deg p_i(x) + \lambda_\infty .$$

However,

$$d(x) = \prod_{i=1}^{l} p_i(x)^{\lambda_i};$$

$$\lambda_\infty = \begin{cases} \deg n(x) - \deg d(x), & \text{if } \deg n(x) - \deg d(x) > 0, \\ 0, & \text{if } \deg n(x) - \deg d(x) \leqslant 0. \end{cases}$$

This gives

$$\deg N(\alpha) \geqslant \begin{cases} \deg(\prod p_i(x)) + \deg n(x), & \text{if } \deg n(x) - \deg d(x) > 0, \\ \deg(\prod p_i(x)) + \deg d(x), & \text{if } \deg n(x) - \deg d(x) \leqslant 0. \end{cases}$$

This proves part (B).

(C) This is simply an application of Theorems 4 and 10 of [2], when $p^n = 2$ to (1);

$$\deg N(\alpha) = -(2/e_\infty)\, v_{\mathfrak{P}_\infty}(\alpha) \geqslant 2G + 1.$$

This part of the theorem is stated separately only because it is in this form that the theorem will be used. This completes the proof of Theorem 4.

COROLLARY. *If K is an imaginary quadratic extension of $k(x)$ for which the null class group has exponent 2, then, for any prime $\mathfrak{p}$ of $k(x)$ which splits in K,*

$$\deg_{k(x)} \mathfrak{p} > G/f_\infty ,$$

where G is the genus of K and f_∞ is the degree of the prime of K over the infinite prime of $k(x)$.

Proof. Let $p(x)$ be the polynomial prime of $k[x]$ associated with the divisor prime $\mathfrak{p}$, and let $\mathfrak{P}_1$ be either prime of K which lies over $\mathfrak{p}$. Thus,

$$\mathfrak{P}_1^{\deg \mathfrak{P}_\infty}/\mathfrak{P}_\infty^{\deg \mathfrak{p}} \in D_0(K).$$

Now since the exponent of the null class group is 2,

$$(\mathfrak{P}_1^{f_\infty}/\mathfrak{P}_\infty^{\deg \mathfrak{p}})^2 = (\alpha), \qquad \alpha \in K.$$

Taking norms of both sides gives

$$(\mathfrak{p}^{f_\infty}/\mathfrak{p}_{1/x}^{f_\infty \deg \mathfrak{p}})^2 = (N(\alpha)).$$

But then,

$$N(\alpha) = a \cdot p(x)^{2f_\infty}$$

for some $a \in k$. By part (C) of the theorem,

$$2f_\infty \deg p(x) \geqslant 2G + 1.$$

Thus

$$\deg \mathfrak{p} > G/f_\infty .$$

This proves the corollary.

This leads to the proof of Theorem 2.

Proof. Now, K is a quadratic extension of $k(x)$ for which the null class group has exponent 2. Suppose there is a prime of degree 1 in $k(x)$ which splits in K; let it be the infinite prime of $k(x)$. Then, if $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are 2 primes of K which lie over the infinite prime of $k(x)$,

$$\mathfrak{P}_1/\mathfrak{P}_2 \in D_0(K).$$

Therefore,

$$\mathfrak{P}_1^2/\mathfrak{P}_2^2 = (\alpha),$$

and, by [2, Theorems 4 and 10],

$$2 \geqslant G + \tfrac{1}{2},$$
$$G \leqslant \tfrac{3}{2}.$$

Thus, if a prime of degree 1 splits in such a K, K has genus 1.

Next, suppose all the primes of degree 1 in $k(x)$ split in K; then K has genus 1 and has $2q + 2$ primes of degree 1, where $| k | = q$. However, by the Riemann hypothesis,

$$|(2q + 2) - (q + 1)| \leqslant 2q^{1/2},$$

or equivalently,

$$q - 2q^{1/2} + 1 \leqslant 0.$$

This cannot happen for $q > 1$. So some prime of degree 1 in $k(x)$ must not split in K, and this concludes the proof.

3. Proof of Theorem 3

The first step in the proof of Theorem 3 is to establish an upper bound on the order of constant field of a congruence function field with null class exponent 2. This bound is furnished by a well-known result in algebraic geometry. From algebraic geometry, it is known that the p rank of the null class group of an algebraic function field over an algebraically closed field of constants is $2G$, if p is not the characteristic, and is at most G when p is the characteristic. Thus in a congruence function field the 2 rank of the null class group is at most $2G$ when 2 is not the characteristic and at most G when 2 is the characteristic. This gives immediately,

Lemma 1. *If K/k is a congruence function field in which the null class group has exponent* 2, *then*

$$| k | = q = 2, 3, 4, 5, 7, \text{ or } 9.$$

Proof. If k has odd characteristic, then for h, the class number of K,

$$h \leqslant 2^{2G},$$

since $C_0(K)$ is at most the product of $2G$ copies of $\mathbb{Z}_2$. However, by the Riemann hypothesis,

$$(q^{1/2} - 1)^{2G} \leqslant h \leqslant 2^{2G}.$$

This implies

$$q \leqslant 9.$$

If k has characteristic 2, then

$$(q^{1/2} - 1)^{2G} \leqslant h \leqslant 2^{G},$$

or, equivalently

$$q \leqslant 6.$$

This proves the lemma.

Now, returning to the proof of Theorem 3, if K is an extension of $k(x)$ which has null class exponent 2, then by Theorem 2, there is some prime of degree 1 in $k(x)$ which does not split in K. If, further, K is such that not all the primes of degree 1 of $k(x)$ are inert in K and such that the genus $G > 1$, then

some prime of degree 1 must ramify. Thus it can be assumed that the K in Theorem 3 is imaginary and that the infinite prime of $k(x)$ ramifies in K. Now under this assumption, the corollary to Theorem 4 says that no prime of degree G or less can split in K. However, this fact together with the techniques employed in the proof of Theorem 6 of [2] gives that if the genus of K is odd and

$$q^G - 2Gq^{G/2} + 1 > GR,$$

where R is the number of primes of $k(x)$ that ramify in K, then there is a prime of degree at most G which splits in K. Thus K could not have genus G.

Case i. $q = 9$. The number of primes of $k(x)$ which ramify in K is less than or equal to $2G + 2$ (the degree of the discriminant by the genus formula). Thus the genus G cannot be odd and satisfy

$$9^G - 2 \cdot G \cdot 3^G + 1 > G(2G + 2).$$

Thus, if the genus of K is odd it must be 1; for, when $G = 3$,

$$9^3 - 2 \cdot 3 \cdot 3^3 + 1 = 568 > 24 = 3(6 + 2).$$

If G is even it cannot satisfy the inequality

$$9^{G-1} - 2 \cdot G \cdot 3^{G-1} + 1 < (G - 1)(2G + 2),$$

and then it must be 2; for if $G = 4$

$$9^3 - 2 \cdot 4 \cdot 3^3 + 1 = 514 > 30 = 3(8 + 2).$$

Thus, if $q = 9$, the genus of K must be 1 or 2. Further analysis rules out the case of genus 2; for by (2) the class number of K with genus 2 is 2, 4, 8, or 16. Also by Lemma 1, there can be no prime of degree 1 or 2 which splits in K. Let M_i be the number of primes of $k(x)$ of degree i which ramify in K, and let N_i be the number of primes of K of degree i. By the genus formula for $G = 2$,

$$0 \leqslant m_1 + 2M_2 \leqslant \deg \delta = 6. \tag{3}$$

Also, since no prime of degree 1 or 2 splits in K,

$$\begin{aligned} N_1 &= M_1\,; \\ N_2 &= M_2 + (q + 1) - M_1\,. \end{aligned} \tag{4}$$

The zeta function $L(u)$ of K is given by (see [3, p. 427]),

$$\begin{aligned} L(u) = 1 &+ (N_1 - (q + 1))\,u + \tfrac{1}{2}(N_1^2 - N_1 - 2qN_1 + 2N_2 + 2q)\,u^2 \\ &+ q(N_1 - (q + 1))\,u^3 + q^2u^4, \end{aligned}$$

and plugging (4) and (5) into $L(1)$ gives

$$h = 1 + \tfrac{1}{2}(M_1^2 - M_1) + M_2\,, \tag{6}$$

which is independent of q.

In this particular case where $q = 9$, the Riemann hypothesis gives

$$(1 - q^{1/2})^4 = 16 \leqslant h.$$

Thus h must be 16. There is, however, only one simultaneous solution for (3) and (6) for $h = 16$; this is $M_1 = 6$ and $M_2 = 0$. In this case the zeta function must be

$$L(u) = 1 - 4u - 26u^2 - 36u^3 + 81u^4.$$

However, by the Riemann hypothesis the reciprocals of the roots of $L(u)$ are $3e^{\pm i\theta_1}$, $3e^{\pm i\theta_2}$, and thus

$$\begin{aligned} L(u) &= (1 - 3e^{i\theta_1}u)(1 - 3e^{-i\theta_1}u)(1 - 3e^{i\theta_2}u)(1 - 3e^{-i\theta_2}) \\ &= (1 - 6\cos\theta_1 u + 3u^2)(1 - 6\cos\theta_2 u + 3u^2). \end{aligned}$$

Therefore,

$$\begin{aligned} \cos\theta_1 + \cos\theta_2 &= 2/3, \\ \cos\theta_1 \cos\theta_2 &= -11/9, \end{aligned}$$

and so $\cos\theta_1$ and $\cos\theta_2$ are roots of the equation

$$x^2 - (2/3)\,x - (11/9) = 0.$$

The roots of this equation are not both between -1 and 1. There is no field of the proper type with $q = 9$, $G = 2$.

Case ii. $q = 7$. Again if G is the genus of K, there are at most $2G + 2$ primes of $k(x)$ that ramify in K. Thus G cannot be odd and satisfy

$$7^G - 2G7^{G/2} + 1 > G(2G + 2).$$

Then if G is odd, it must be 1, for $G = 3$ satisfies this inequality. If G is even it must be 2 because $G = 4$ satisfies

$$7^{G-1} - 2G7^{G-1/2} + 1 > (G - 1)(2G + 2).$$

Now in this case where $q = 7$, the Riemann hypothesis gives

$$h \geqslant (1 - 7^{1/2})^4 \sim 7.1,$$

and so $h = 8$ or 16. There is only one simultaneous solution of (3) and (6)

each for $h = 8$ and $h = 16$. These solutions and the zeta functions they imply are:

$h = 16;\quad M_1 = 6,\quad M_2 = 0,\quad L(u) = 1 - 2u - 18u^2 - 14u^3 + 49u^4,$

$h = 8;\quad M_1 = 4,\quad M_2 = 1;\quad L(u) = 1 - 4u - 10u^2 - 28u^3 + 49u^4.$

However, the same methods used above show that these cannot be the zeta functions of congruence function fields. Thus if $q = 7$, then $G = 1$.

Case iii. $q = 5$. There are at most $2G + 2$ primes of $k(x)$ that ramify in K. If G is odd, it cannot satisfy

$$5^G - 2 \cdot G \cdot 5^{G/2} + 1 > G(2G + 2),$$

and must therefore be 1. Similarly if G is even it must be 2. Thus if $q = 5$, then $G \leqslant 2$.

Case iv. $q = 4$. In this case $K/k(x)$ is an Artin–Schreier extension, and so all ramification must be wild. This allows a better estimate on the number of primes $k(x)$ that ramify in K. If $G = 3$, the degree of the discriminant is 8. Now since the ramification is wild, each prime that appears in the discriminant has a power of at least 2. Thus, there are at most four primes of $k(x)$ that ramify in K. But,

$$4^3 - 2 \cdot 3 \cdot 2^3 + 1 = 17 > 12 = 3 \cdot 4.$$

And so there is no congruence function field of the proper type of odd genus larger than 1.

If G is even, consider $G = 6$. The degree of the discriminant is 14, and thus there are at most six primes of $k(x)$ which ramify in K (six since there are only five primes of degree 1 in $k(x)$). Then

$$4^5 - 2 \cdot 6 \cdot 2^5 + 1 > 5 \cdot 6.$$

Both of these facts together give that, when $q = 4$, G must be 1, 2, or 4. Further analysis of the type used in the case of $q = 9$, $G = 2$ rules out $G = 4$. There are 13 possible combinations of ramified primes which give a power of 2 for the class number. These can all be eliminated by studying the zeta functions they imply. And so, $q = 4$ implies $G = 1$ or 2.

Case v. $q = 3$. In this case a more accurate approximation of the number of primes that ramify is needed. If $G = 5$, then the degree of the discriminant is 12. There are, however, only four primes of degree 1 in $k(x)$. Thus there are at most eight primes of $k(x)$ that ramify in K, four of degree 1, and four of degree 2. However,

$$3^5 - 2 \cdot 5 \cdot 3^{5/2} + 1 > 5 \cdot 9.$$

Thus if $q = 3$, then $G \leqslant 4$.

Case vi. $q = 2$. This is an Artin–Schreier case, so all the ramification is wild. In this case a similar procedure gives $G \leqslant 8$. This completes the proof of Theorem 3.

The restriction on the primes of degree 1 in the statement of Theorem 3 is redundant when $q = 7$ and $q = 9$. In a quadratic extension K of $k(x)$ in which the null class group has exponent 2, all the classes in this group are ambiguous, i.e., they are fixed by the action of the Galois group of $K/k(x)$. Thus the class number h of K is equal to the ambiguous class number h_0. There is a well-known theorem of Schmidt (see [4, p. 69]) which can be used to calculate the ambiguous class number of K. In particular, when K is a geometric quadratic extension of $k(x)$ which has null class exponent 2 and in which all the primes of degree 1 of $k(x)$ are inert,

$$h = h_0 \leqslant 2^{l-1},$$

where l is the number of primes in $k(x)$ which ramify in K. If G is the genus of K, the genus formulas show that the degree of the discriminant is $2G + 2$. Since no prime of degree 1 in $k(x)$ ramifies in K,

$$l \leqslant G + 1;$$
$$\therefore \quad h \leqslant 2^G.$$

Now, by the Riemann hypothesis,

$$(1 - q^{1/2})^{2G} \leqslant h \leqslant 2^G,$$

or equivalently,

$$q \leqslant 3 + 8^{1/2} < 6.$$

References

1. R. E. MacRae, On unique factorization in certain rings of algebraic functions, *J. Algebra* **17** (1971), 243–261.
2. M. L. Madan and D. J. Madden, The exponent of class groups in congruence function *fields*, *Acta Arith.* **32** (1976).
3. M. L. Madan and C. S. Queen, Algebraic function fields of class number one, *Acta Arith.* **20** (1972), 423–432.
4. M. Moriya, Rein arithmetisch-algebraischer Aufbau der Klassenkörper theorie über algebraischen Funktionenkörpern einer Unbestimmten mit endlichem Konstantenkörper, *Japan J. Math.* **15** (1938), 67–84.